IoT TEXNOLOGIYALARI YORDAMIDA AQLLI BINOLARDA MAXFIYLIKNI TA'MINLASH

Kuchaboyev Ruslan Tellayevich, *Toshkent Axborot texnologiyalari universiteti Qarshi filiali katta o'qituvchisi*

Annotatsiya. *Ushbu maqolada IoT texnologiyalarining asosiy tushunchalari, aqlli binolarda maxfiylikni ta'minlash usullari, muammo va yechimlari, xavfsizlikni ta'minlash mexanizmlari hamda IoT kontekstida ma'lumotlar maxfiyligi va standartlashtirish tamoyillari ochib berilgan hamda aqlli binolarning afzalliklari va samaradorligi keltirilgan.*

Kalit so'zlar: *IoT texnologiyalar, maxfiylikni taminlash, aqlli bino, IoT konteksti, ma'lumotlar maxfiyligi, xavfsizlikni ta'minlash.*

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ В УМНЫХ ЗДАНИЯХ С ИСПОЛЬЗОВАНИЕМ IoT-ТЕХНОЛОГИЙ

Кучабоев Руслан Теллаевич, *Старший преподаватель Каршинского филиала Ташкентского университета информационных технологий*

Аннотация: *В статье раскрыты основные концепции технологий Интернета вещей, методы защиты конфиденциальности, проблемы и решения в умных зданиях, механизмы безопасности, а также принципы конфиденциальности и стандартизации данных в контексте Интернета вещей, а также преимущества и эффективность умных зданий.*

Ключевые слова: *IoT технологии, конфиденциальность, умное здание, IoT контекст, конфиденциальность данных, безопасность.*

ENSURING PRIVACY IN SMART BUILDINGS USING IoT TECHNOLOGIES

Kuchaboyev Ruslan Tellayevich, senior lecturer of the Karshi branch of the Tashkent University of Information Technologies

Annotation: *The article reveals the basic concepts of Internet of Things technologies, methods for protecting privacy, problems and solutions in smart buildings, security mechanisms, as well as principles of confidentiality and data standardization in the context of the Internet of Things, as well as the advantages and efficiency of smart buildings.*

Keywords: *IoT technologies, privacy, smart building, IoT context, data privacy, security.*

Raqamlashayotgan jamiyatga o’tish jarayonida insonlar yashaydigan uyning ichi va atrofida integrallashgan infrastruktura yaratilib, ushbu infrastruktura vositasida axborot servislari va aloqa kanallariga ega bo’lib bormoqda. Bunday imkoniyatlar uydagi va ish joyidagi axborot ta’minotlari orasidagi chegarani yo’qotib, ularni bir butun tuzimga aylantiradi. Integrallashgan tizimda bunday binolarga o’rnatiladigan maxsus kompyuterlar maishiy texnika, isitish tizimi, himoya tizimi kabi barcha zarur qurilmalar ishini maxsus dastur orqali boshqarib turadi. Shuningdek tizim suv, elektr, gaz va boshqa resurslar sarfi to’g’risida ma’lumot to’plab boradi va to’lovlar xajmi haqida axborotlarni taqdim etadi. Bunday binolar “aqlli bino”lar deb ataladi.

Maxfiylikni saqlash aqlli binolarda ishlatiladigan IoT kontekstida juda muhimdir. Aqlli binolarda IoT qurilmalari va texnologiyalarining tobora ko'payib borishi bilan ushbu qurilmalar tomonidan to'plangan va uzatiladigan ma'lumotlarning maxfiyligi va xavfsizligi haqida xavotir kuchaymoqda.

Internet uskunalari (inglizcha: *internet of things*, *IoT*) - bu bir-biri bilan yoki tashqi muhit bilan o‘zaro ta’sir qilish uchun o‘rnatilgan vositalar va texnologiyalar bilan jihozlangan jismoniy obyektlar (“*narsalar”*) o‘rtasida ma’lumotlarni uzatish tarmog‘i tushunchasi. Bunday tarmoqlarni tashkil etish iqtisodiy va ijtimoiy jarayonlarni qayta qurish, ba’zi harakatlar va operatsiyalarda inson ishtirokiga bo‘lgan ehtiyojni yo‘q qilishga qodir.

Ma’lumotlar tarmoqlariga ulanish vositalari bilan ta’minlanmagan jismoniy dunyo obyektlarining “buyumlar interneti”ga jalb etilishi ushbu obyektlarni

(“narsalar”) identifikatsiyalash texnologiyalaridan foydalanishni talab qiladi. RFID texnologiyasi konsepsiyaning paydo bo‘lishiga turtki bo‘lgan bo‘lsa-da, avtomatik identifikatsiya qilish uchun ishlatiladigan barcha vositalar bunday texnologiyalar sifatida ishlatilishi mumkin: optik jihatdan tanib olinadigan identifikatorlar (shtrix kodlari, Data Matrix, QR kodlari), real vaqtda joylashuvni aniqlash vositalari. “Buyumlar interneti”ning har tomonlama tarqalishi bilan obyekt identifikatorlarining o‘ziga xosligini ta’minlash muhim ahamiyatga ega, bu esa o‘z navbatida standartlashtirishni talab qiladi.

Internet tarmoqlariga ulangan obyektlar uchun an’anaviy identifikator tarmoq adapterining MAC manzili bo‘lib, u sizga ulanish darajasida qurilmani aniqlash imkonini beradi, shu bilan birga mavjud manzillar diapazoni deyarli tugamaydi (MAC-48 da 2^{48} manzil). Bunday qurilmalar uchun kengroq identifikatsiya qilish imkoniyatlari IPv6 protokoli bilan ta’minlanadi, u yer aholisiga kamida 300 million qurilmani noyob tarmoq qatlami manzillari bilan ta’minlaydi.

O‘lchash vositalari tashqi muhit haqidagi ma’lumotlarni mashina o‘qiy oladigan ma’lumotlarga aylantirishni ta’minlovchi va shu orqali hisoblash muhitini mazmunli ma’lumotlar bilan to‘ldirishni ta’minlovchi “Buyumlar Interneti”da alohida o‘rin tutadi. Elementar datchiklardan (masalan, harorat, bosim, yorug‘lik), iste’molni o‘lchash asboblaridan (masalan, aqlli hisoblagichlar) murakkab integratsiyalashgan o‘lchash tizimlarigacha bo‘lgan keng turdagi o‘lchov asboblari qo‘llanadi. “Buyumlar interneti” konsepsiyasi doirasida o‘lchash vositalarini tarmoqda (masalan, simsiz sensor tarmoqlari, o‘lchash komplekslari) birlashtirish muhim ahamiyatga ega, buning natijasida mashinadan mashinaga o‘zaro ta’sir qilish tizimlarini qurish mumkin.

Mumkin bo‘lgan ma’lumotlarni uzatish texnologiyalari spektri simsiz va simli tarmoqlarning barcha mumkin bo‘lgan vositalarini qamrab oladi. Simsiz ma’lumotlarni uzatish uchun past tezlikda samaradorlik, nosozliklarga chidamlilik, moslashuvchanlik va o‘zini-o‘zi tashkil qilish imkoniyati kabi fazilatlar “buyumlar interneti”ni yaratishda ayniqsa muhim rol o‘ynaydi. Ushbu quvvatga asosiy

qiziqish IEEE 802.15.4 standarti bo‘lib, u energiya tejaydigan shaxsiy tarmoqlarni tashkil qilish uchun jismoniy qatlam va kirishni boshqarishni belgilaydi va ZigBee, WirelessHart, MiWi, 6LoWPAN, LPWAN kabi protokollar uchun asos hisoblanadi.

IoT-dagi maxfiylik shaxsiy ma'lumotlarni himoya qilish va IoT qurilmalari va tizimlari tomonidan ushbu ma'lumotlarni to'plash, saqlash va ulardan foydalanishni nazorat qilishni anglatadi. Bu shaxslarning shaxsiy ma'lumotlari qanday to'planishi, qayta ishlanishi va almashilishini aniqlash huquqiga ega bo'lishini ta'minlashni o'z ichiga oladi.

IoT-dagi maxfiylik turli jihatlarni o'z ichiga oladi, jumladan:

- ma'lumotlarning maxfiyligi;
- foydalanuvchi maxfiyligi;
- joylashuv maxfiyligi.

IoT-dagi maxfiylik bir nechta qiyinchiliklar va xavflarga duch keladi:

ma'lumotlarning buzilishi

ma'lumotlarning tarqalishi

shaffoflikning yo'qligi

IoT-da maxfiylik bilan bog'liq muammolar va xavflarni bartaraf etish uchun maxfiylikni saqlashning turli usullari qo'llaniladi, jumladan:

- Ma'lumotlarni anonimlashtirish va taxalluslash;
- Shifrlash va xavfsiz aloqa protokollari;
- Kirishni boshqarish va autentifikatsiya qilish mexanizmlari;
- Maxfiylikni oshirish texnologiyalari (uy hayvonlari);
- Dizayn bo'yicha maxfiylik.

Dizayn bo'yicha maxfiylik quyidagi printsiplarga asoslanadi:

- Proaktiv reaktiv emas;
- Maxfiylik standart Sozlama sifatida;
- To'liq funksionallik;
- Xavfsizlik.

IoT tizimini loyihalash va ishlab chiqishda maxfiylik masalalarini kiritish uchun quyidagi amaliyotlarga amal qilinadi:

- maxfiylik xavfini aniqlash va kamaytirish uchun maxfiylik ta'sirini baholashni o'tkazish.
- ma'lumotlarni yig'ish va ulardan foydalanish to'g'risida shaxslarni xabardor qilish uchun maxfiylik siyosati va rozilik mexanizmlarini amalga oshirish.
- shaxsiy ma'lumotlarni boshqarish uchun foydalanuvchilarga yo'naltirilgan maxfiylikni boshqarish vositalari va interfeyslarini taqdim etish.

IoT-ning asosiy muammolaridan biri bu IoT qurilmalari va ma'lumotlariga ruxsatsiz kirishdir. Bu maxfiylikning buzilishiga olib kelishi va butun tizim xavfsizligini buzishi mumkin.

Ushbu muammoni hal qilish uchun parollar, biometrikalar va ikki faktorli autentifikatsiya kabi kuchli autentifikatsiya mexanizmlari amalga oshiriladi. IOT qurilmalari va ma'lumotlariga ruxsatsiz kirishni cheklash uchun kirishni boshqarish mexanizmlari ham qo'llaniladi.

Transport qatlami xavfsizligi (TLS) kabi xavfsiz aloqa protokollari IoT qurilmalari va tizimlari o'rtasida uzatiladigan ma'lumotlarning shifrlanganligini va ularni ushlab qolish yoki buzish mumkin emasligini ta'minlash uchun ishlatiladi.

Ma'lumotlarning tarqalishi va maxfiylikning buzilishi IoTda muhim tashvishlardir, chunki ular shaxsiy ma'lumotlarning ruxsatsiz oshkor qilinishiga olib kelishi mumkin.

Ma'lumotlarning tarqalishi va maxfiylikning buzilishi xavfini kamaytirish uchun ma'lumotlarni anonimlashtirish va taxalluslash texnikasi qo'llaniladi. Ushbu texnikalar shaxsan aniqlanadigan ma'lumotlarni olib tashlaydi yoki o'zgartiradi, bu esa ma'lumotlardan shaxslarni bevosita aniqlab bo'lmasligini ta'minlaydi.

IOT-da ma'lumotlar maxfiyligini himoya qilish uchun differentsial maxfiylik va homomorfik shifrlash kabi maxfiylikni oshiruvchi texnologiyalar qo'llaniladi. Ushbu texnologiyalar maxfiylikni saqlagan holda ma'lumotlarni tahlil qilish va qayta ishlash usullarini taqdim etadi.

Iotda shaxslar ko'pincha shaxsiy ma'lumotlarini to'plash va ulardan foydalanish ustidan cheklangan ko'rish va nazoratga ega.

Ushbu muammoni hal qilish uchun maxfiylik siyosati va rozilik mexanizmlari amalga oshiriladi. Maxfiylik siyosati shaxslarni IoT qurilmalari va tizimlaridan ma'lumotlarni yig'ish va ulardan foydalanish amaliyoti to'g'risida xabardor qiladi. Rozilik mexanizmlari jismoniy shaxslarga shaxsiy ma'lumotlarini to'plash va ulardan foydalanish uchun xabardor rozilik berishga imkon beradi.

Shaxsiy ma'lumotlarni boshqarish uchun foydalanuvchilarga yo'naltirilgan maxfiylikni boshqarish vositalari va interfeyslari ishlab chiqilgan. Ushbu vositalar shaxslarga maxfiylik imtiyozlarini boshqarish, ma'lumotlarni yig'ish amaliyotini ko'rib chiqish va shaxsiy ma'lumotlari bo'yicha o'z huquqlaridan foydalanishga imkon beradi.

Aqlli binolarni avtomatlashtirish tizimlari yoritish, isitish, shamollatish va havoni tozalash (HVAC) va xavfsizlik kabi turli xil qurilish funktsiyalarini avtomatlashtirish va optimallashtirish uchun IoT texnologiyalaridan foydalanadi. Maxfiylikni saqlash texnikasi ushbu tizimlarda bino aholisining maxfiyligini himoya qilish uchun juda muhimdir.

Aqlli binolarni avtomatlashtirish tizimlarida maxfiylikni saqlash texnikasiga quyidagilar kiradi:

- Qurilish tizimlariga ruxsatsiz kirishni cheklash uchun kirishni boshqarish mexanizmlarini amalga oshirish.

- Qurilmalar o'rtasida uzatiladigan ma'lumotlarni himoya qilish uchun shifrlash va xavfsiz aloqa protokollaridan foydalanish.
- Bino egalarining maxfiyligini ta'minlash uchun ma'lumotlarni anonimlashtirish va taxalluslashtirish texnikasidan foydalanish.

Aqlli binolarda maxfiylikni saqlashning bir misoli maxfiylikni saqlaydigan energiya boshqaruvidir. IoT qurilmalari va ma'lumotlar tahlilidan foydalangan holda, aqlli binolar bino aholisining maxfiyligini saqlab, energiya sarfini optimallashtirishi mumkin. Bunga ma'lumotlarni anonimlashtirish texnikasi va xavfsiz aloqa protokollaridan foydalanish orqali erishiladi.

Aqlli binoning afzalliklari samaradorlikni oshirishi, energiya sarfini kamaytirishi va operatsion xarajatlarni kamaytirishi mumkin. Bundan tashqari, u sizning biznesingizning mahalliy iqtisodiyotini yaxshilashga yordam beradi. Jamiyat haqida noyob ma'lumotlarni to'plash orqali aqlli binolar ishlab chiquvchilarga shahringizda qanday qilib yaxshiroq biznes qilishni tushunishga yordam beradi. Ushbu ma'lumotlar biznesingizni yanada samarali qilish uchun ishlatilishi mumkin. Bu sizning biznesingiz uchun daromad va foydaning oshishiga olib keladi.

Aqlli binolardan hosildorlikning oshishi shunchaki nazariya emas. Aqlli bino tomonidan to'plangan ma'lumotlar biznes maqsadlari va vazifalarini yaratish uchun ishlatilishi mumkin. Masalan, u biznes rahbarlariga yig'ilish zalida nechta odam borligini yoki ular bino ichida joylashganligini aytishi mumkin. Ushbu ma'lumotlar foydalanuvchi tajribasini va kompaniyaning umumiy samaradorligini oshirish uchun ishlatilishi mumkin. Bundan tashqari, aqlli binolar ko'chmas mulk xarajatlarini kamaytirishi mumkin. Bu aqlli binolarning biznes olamiga taqdim etadigan afzalliklaridan bir nechtasi.

Aqlli binoning eng foydali xususiyatlaridan biri uning bandlik darajasini aniqlash qobiliyatidir. Ushbu ma'lumot binolar menejerlariga energiya sarfini 10 foizga kamaytirishga yordam beradi. Ushbu texnologiya shuningdek, chiqindilarni kamaytirishi va atrof-muhitning barqarorligini yaxshilashi mumkin. Aqlli bino boshqaruvlari ish haqini pasaytirish va ofis binolarida energiyani tejash uchun

ajoyib yechimdir. Ushbu tizim binoning ehtiyojlariga moslashtirilishi mumkin, bu bino menejerlariga operatsiyalarni optimallashtirish va keraksiz energiya sarfini kamaytirish imkonini beradi.

Ob'ektning ishlashini optimallashtirish orqali aqlli qurilish texnologiyasi xarajatlarni kamaytiradi va ishlab chiqarishni oshiradi. Kommunal xarajatlar ob'ektni ishlatish xarajatlarining eng katta qismi bo'lib, undan keyin texnik xizmat ko'rsatish va tozalash xarajatlari turadi. Aqlli qurilish texnologiyasidan foydalangan holda, ob'ektlar rahbarlari o'z jamoalarining samaradorligini oshirish va samaradorligini oshirish bilan birga pulni tejashlari mumkin. Qurilish operatsiyalarini avtomatlashtirish orqali ob'ektlar rahbarlari o'z xodimlarining qo'l mehnatiga sarflagan vaqtini minimallashtirishi va muhimroq vazifalarga e'tibor qaratishlari mumkin.

Xulosa o’rnida shuni ta’kidlashimiz mumkinki, aqlli binolar ham ekologik jihatdan qulayroqdir, chunki ular energiya ishlab chiqarish tizimlariga ega. Bu tizimlar iste'mol qilganingizdan ko'ra ko'proq energiya ishlab chiqarishga yordam beradi va hatto elektr uzilishlari xavfini kamaytiradi. Bundan tashqari, ular sizning ish joyingizni yanada qulayroq qilishlari va xodimlaringizning mamnunligini oshirishlari mumkin. Biznes egasi sifatida ushbu imtiyozlar sizga xarajatlarni kamaytirishga va sayyorani tejashga yordam beradi.

Foydalanilgan adabiyotlar:

1. Uzakov, O. S., Raxmatullayev, D. A., Bekmatov, A. K., & Dilmurodov, Z. D. (2023). IOT TEXNOLIGIYALARI XAVFSIZLIGIDA SMART HOUSELARNI MOBIL QURILMALAR YORDAMIDA BOSHQARISH. ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ, 23(7), 105-107.
2. Карачев О. Интернет вещей: что это и с чем его едят // Chëza. 2016. URL: http://chezasite.com/news/chto-takoeinternet-veshei-82180.html

3. Портер М., Хеппельман Дж. Революция в конкуренции. "Умные" технологии изменяют конкурентную борьбу // Harvard Business Review. 2016. URL: http://hbr-russia.ru/special/ptc-iot/
4. Shukrullaevna, N. D., & Bahodirivich, R. A. (2017). Improving the quality on line learning process with MOOC. *Academy*, *2*(6 (21)), 21-24.
5. Normurodov, A. D., & Rustamov, A. B. (2023). INTERNET-BUYUMLAR IOT AFZALLIKLARI VA XAVFSIZLIK MUAMMOLARI. *INNOVATSION IQTISODIYOTNI SHAKLLANTIRISHDA AXBOROT KOMMUNIKATSIYA TEXNOLOGIYALARINING TUTGAN O 'RNI*, *1*(1).
6. Normurodov, A. D., & Rustamov, A. B. (2023). INTERNET OF THINGS CYBER THREATS AND THEIR MANAGEMENT IN IoT. *INNOVATSION IQTISODIYOTNI SHAKLLANTIRISHDA AXBOROT KOMMUNIKATSIYA TEXNOLOGIYALARINING TUTGAN O 'RNI*, *1*(1).
7. Бекматов А.К., Кутдусова Э.Р., Мукимов Ш.И., & Давлатова Н.Н. (2023). ПРОГРЕССИВНЫЕ ТЕНДЕНЦИИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Экономика и социум, (6-1 (109)), 1264-1270.
8. Бекматов, А. К., Кутдусова, Э. Р., & Муқимов, Ш. И. (2023). ПРЕИМУЩЕСТВА И ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СФЕРЕ. O'ZBEKISTONDA FANLARARO INNOVATSIYALAR VA ILMIY TADQIQOTLAR JURNALI, 2(20), 280-286.